TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 02/12 pp121-132
Volume 19, Number 2, April 2014

Electricity Services Based Dependability Model of Power Grid Communication Networking

Jiye Wang, Kun Meng*, Junwei Cao, Zhen Chen, Lingchao Gao, and Chuang Lin

Abstract: The technology of Ultra-High Voltage (UHV) transmission requires higher dependability for electric power grid. Power Grid Communication Networking (PGCN), the fundamental information infrastructure, severs data transmission including control signal, protection signal, and common data services. Dependability is the necessary requirement to ensure services timely and accurately. Dependability analysis aims to predicate operation status and provide suitable strategies getting rid of the potential dangers. Due to the dependability of PGCN may be affected by external environment, devices quality, implementation strategies, and so on, the scale explosion and the structure complexity make the PGCN's dependability much challenging. In this paper, with the observation of interdependency between power grid and PGCN, we propose an electricity services based dependability analysis model of PGCN. The model includes methods of analyzing its dependability and procedures of designing the dependable strategies. We respectively discuss the deterministic analysis method based on matrix analysis and stochastic analysis model based on stochastic Petri nets.

Key words: power grid communication networking; dependability; stochastic Petri nets; strategy design

1 Introduction

Dependability reflects the ability that a system works well under given loads, and it was determined comprehensively by system's internal feature and potential work loads[1]. Dependability analysis is a loop of evaluating current status, computing improvement strategies, implementation, and reevaluation, and aims to construct appreciate models supporting the above procedure[2]. At present, pursuing more robust and intelligent power grid is the main goal of power grid operation enterprises, such as State Grid Company of China (SGCC) has planned to invest 1.6 trillion RMB to build the robust smart grid. More information technology will be applied to improve the intelligence of the power grid, though Supervisory Control and Data Acquisition (SCADA) devices have been deployed in recent power transmission systems. As a result, the power grid is evolving into a critical Cyber-Physical System (CPS)[3,4], and many necessary requirements have to be discussed[5-7].

The Power Grid Communication Networking (PGCN) is in charge of transmitting data to desired destinations to support the power grid services, faces challenge to ensure data transmission timely and accurately[8-10]. In other words, the information infrastructure is supporting the control, monitoring,

• Jiye Wang and Lingchao Gao are with Department of Information and Communication, State Grid, Beijing 100031, China. E-mail: jywang@sgcc.com.cn; lingchaogao@sgcc.com.cn.
• Kun Meng is with the Computer School, Beijing Information Science and Technology University, Beijing 100101, China and Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China. E-mail: mengkurt@tsinghua.edu.cn.
• Junwei Cao and Zhen Chen are with the Research Institute of Information Technology, Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beiing 100084, China. E-mail: jcao@tsinghua.edu.cn; zhenchen@tsinghua.edu.cn.
• Chuang Lin is with Department of Computer Science and Technology, Tsinghua University, Beiing 100084, China. E-mail: chlin@tsinghua.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2014-03-18; revised: 2014-03-20

the maintenance, and the exploitation of power supply systems, so power services require information infrastructure more dependable and efficiency, especially for PGCN. The interdependence of them has been studied in literatures[11, 12]. To predicate the status of PGCN and to arrange suitable predetermined strategies are instinctive to enhance its dependability. However, the scale of devices and the diversification of tasks impede the practice evaluating PGCN correctly and timely[13]. To realize the aforementioned goals, Budka et al.[10] discussed the basic design principles based on many kinds of potential applications smart grid should support and suggest a possible architecture. In Ref. [9], many features the system should have are discussed, such as performance, availability, reliability, and security. Niyato et al.[14] gave a reliability analysis method and the optimal design principles for the redundant design. Reference [15] gives reliability analysis model aimed at deployment of communication lines and takes the SONNET for an example to illustrate techniques of modeling, simplification, calculation, and analysis. However, most of current research mainly concentrates the networking structure and the failure of its components instead of considering the interdependence between power grid and PGCN.

This paper focuses on the dependability of PGCN and attempts to present a lightweight evaluation method. On the observation of power grid services bridging the power grid and PGCN, as shown in Fig. 1, we propose the power grid services based model which not only considers the structure features and implementation specifications of PGCN, but also takes account of interdependence of power grid and PGCN.

2 Background

2.1 Smart grid and its communication networking

An electric grid is an interconnected network for delivering electricity power from suppliers to consumers. It consists of power stations generating electricity power, high-voltage transmission lines, and distribution lines. The smart grid is viewed as modernized electrical grid that uses information and communication technology to gather and act on information in an automated fashion to improve the efficiency, reliability, and sustainability of the production and distribution of electricity[3]. Therefore, the smart grid contains the power grid infrastructure and information infrastructure. The power grid infrastructure ensuring electricity power flows safely and efficiently is called the power grid infrastructure. Collecting, transmitting, and processing all kinds of information are tasks of information infrastructure. Control or scheduling centers act as brain of the smart grid and decide feasible strategies of collecting information and implemention control. PGCN conveys a variety of information to ensure performance of the smart grid, and many control centers are connected with PGCN. In a word, the smart grid is a critical CPS. Figure 2 shows a typical structure.

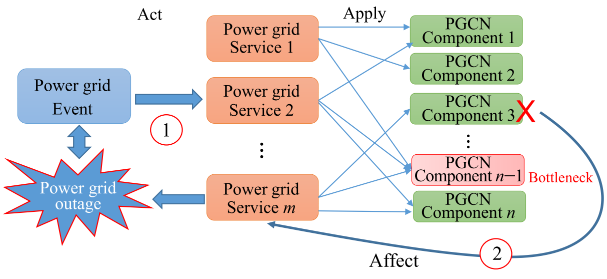

Fig. 1 Interdependence between power grid and PGCN.

As Fig. 1 mentioned, any power grid event will stimulate several power grid services (e.g., relay protection and remote operation), and every power grid service applies a set of PGCN components. Thus, improper configuration will cause performance decrease or non-applicable of PGCN. On the other side, any PGCN component fails may affect the function of some power grid services and cause serious power grid outage.

2.2 PGCN structure and operation specifications

PGCN was built incrementally. Usually, mainstream communication lines are deployed as an ancillary of power lines, and are managed by different administration domains (e.g., national backbone network, area network, and province network) (see Fig. 3). The carriers of PGCN include optical fiber, cable, Power Line (PL), microwave, satellite, etc. Allocation strategies of communication resource are classified into the proactive and reactive. The former reverses resource for special services and the other is not permitted to use, on the contrary, the latter just allocates resource when service arrives. For PGCN of SGCC, the proactive strategies are used extensively. For example, when each power grid service is planned to use a communication line, a 2-Mbit/s bandwidth of this line is reversed to it. The reactive strategies are used

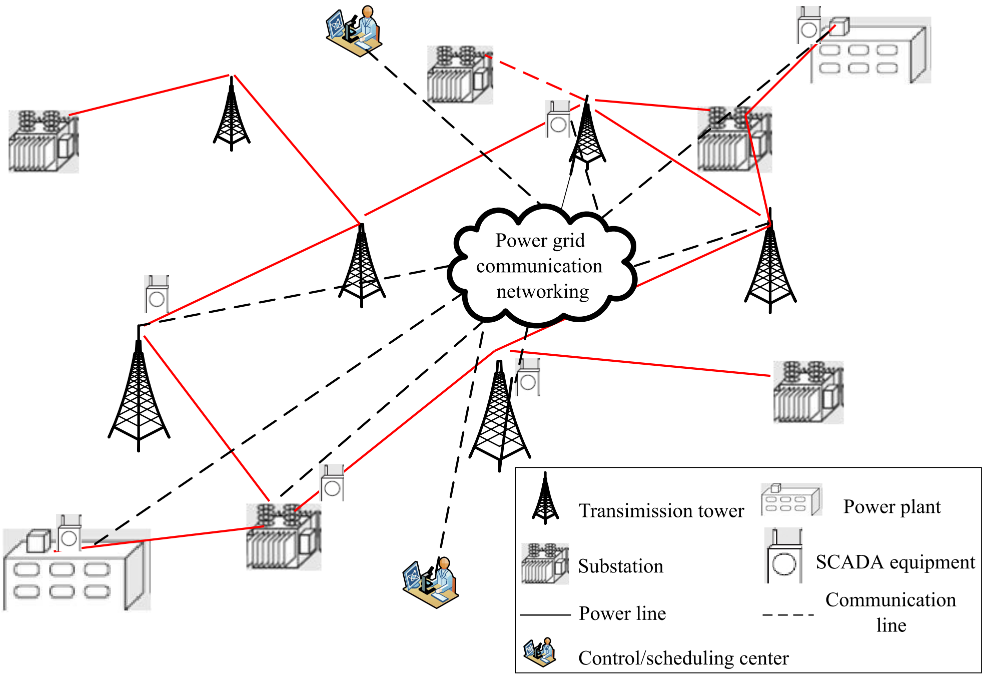

Fig. 2 A typical smart grid structure.

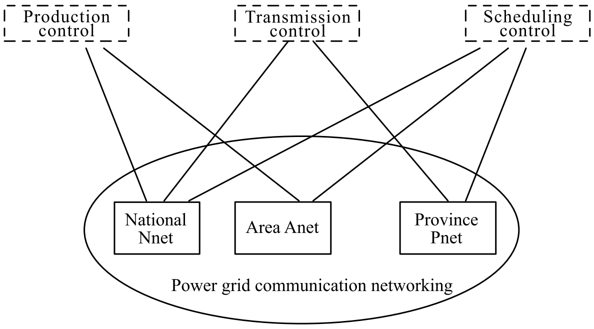

Fig. 3 Administration and operation of PGCN.

for non-power grid services, such as OA system, visual meeting, and so on. Since we aim to study methods to ensure power grid operation, the proactive strategies are assumed to be used in the following analysis.

For sake of security and reliability, every service should be set at least two communication paths they are separated physically. See Fig. 3, for any power grid services, such as production, transmission, and scheduling, it has at least two sets of communication devices. The ordinary backup strategy include MSP1 + 1, SNCP1 + 1, etc.

2.3 Communication patterns of power grid services

The supported power grid services contain production control, transmission control, and power scheduling, and they have various forms, such as voice, control signal, and monitoring information. Production control service aims to adjust workload of power plants according to the predication of consumption in the next period, and keeps balance between supply and consumption. This corresponding communication consists of information collection stage and control signal distribution stage and any fault during the above stages will lead to service outage. This type of service always has different sources and destination nodes. Scheduling control is the process of distributing commands to control devices. Delay and loss of commands will decrease power grid operation performance. Transmission control is in charge of monitoring and regulating power quality of electricity power. The typical service of transmission control includes protection, security, stability control, and so on. PGCN provides functions of direct communication and alarm between devices, sending current status information to the substation or dispatch centers.

For the convenience of description, based on the relationship between the source node and the destination node of information transmission, the service can be divided into direct connect type, relay type, and gathering-feedback type, as shown in Fig. 4. Direct connect type is that existing communication lines between the source and the destination supporting the service. Relay type is that there is no direct communication line, communication between them relies on the intermediate nodes. Gathering-feedback type means that there is

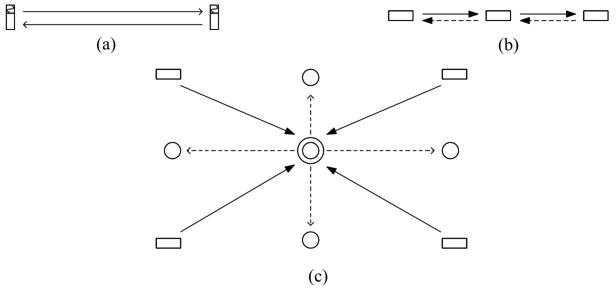

Fig. 4 Types of power grid services: (a) Direct connect type; (b) Relay type; (c) Gathering-feedback type.

only one source or destination node, the relationship of each pair of the source and destination might be direct or relay.

2.4 Dependability impact factors

An undirected graph G may represent a PGCN, and nodes are communication site generating or transmitting data. The edge indicates where there exists channel among sites. In SGCC, the PGCN is a dedicated network with physical isolation, and the Virtual Circuit (VC) is set for every special power grid service. Services have individual requirements for reliability, timeliness, and continuity of transmission. Therefore, the main problems of dependability of PGCN mainly contain disconnection, transmission policy confliction, device failures, and so on[16]. The impact factors include physical environment, service, and management.

(1) Physical factors (such as natural environment and intrinsic properties of device). These factors mainly reflect the impact of the physical properties, including the inherent failure frequency of devices, the deployment policy, and the location[17].

(2) Service factors (such as the burst traffic causing overload and the deployment conflict of services). These factors are caused by lack of enough information, since the construction is always distributedly and incrementally.

(3) Management factors (such as maintenance level, emergency response capability, automation degree, and so on). These factors reflect the impact of the subjective initiatives, compliance with standards is the primary requirement.

The PGCN may be abnormal or failure caused by the combination of several above factors[18]. Failures might be divided into the ordinary, the cascading, and escalating ones. Ordinary failure can be called isolated failure meaning it does cause others. Cascading failure may cause a chain of failures. Escalating failure will become more serious if it was not repaired timely. The failure in PGCN includes line failure and node failure. Line failures break all traffic running on it, and may result in outage or performance decrease of transmission. Node failures imply all devices deployed in this site out of work, will result in all traffic through this site outage.

2.5 Dependability metrics for PGCN

Efficiency, survivability, and invulnerability are studied for dependability analysis of PGCN. From the view of administration, many researchers give dependability metric systems with respect to function layers of PGCN respectively. Concluding the existed results, we propose the PGCN dependability index system including availability, data quality, and maintainability, which reflects the features of leveled indexes and requirement of power grid services. Table 1 shows their relationship.

Formally, availability is defined as the probability of a service was finished within the fixed time interval, if the service is served by the PGCN. The availability is $\mathrm{AC} = \Pr\{t - t_0 \leqslant \delta\}$, where t_0 is the time a power grid service submits the request to PGCN, and t is the time the data arrives at its destination. If $\delta = \infty$, the availability is the probability that no failures occur for nodes and edges. Data quality is measured with bit error ratio, loss ratio of packets, delay, and jitter. The detail can be found in Ref. [2]. Maintainability indicates the ability that a system may find failures and repair them. Mean Time To Repair (MTTR) and fault tolerance degree are two indexes reflecting the maintainability.

3 Electric Services Based Dependability Model of the PGCN

3.1 Overview

Considering comprehensively effect of power grid services, in this part, we propose a model evaluating dependability of PGCNs. We shall discuss quantitative analysis methods from both deterministic and stochastic perspectives, which helps administrators to take reasonable strategies when they are requested to deploy new power grid services.

The dependability model includes the stages of constructing PGCN model, dependability analysis, and judging and computing strategies, as shown in Fig. 5. Network structure, services and management

Table 1 Analysis of dependability metrics of PGCN.

Leveled dependability factors		Service-based dependability metrics		
Layer	Description	Availability	Data quality	Maintainability
Topology	Node invulnerability	+	+	+
	Link invulnerability	+	+	+
Routing	Bandwidth	+	+	
	Delay	+	+	
	Jitter		+	
	Packet loss rate	+	+	
	Throughput	+	+	
Devices	E/M failure rate	+	+	+
	FXO failure rate	+	+	+
	V.24 failure rate	+	+	+
Operation	Natural conditions	+	+	+
	Human factors	+	+	+
	Management	+	+	+
Frequency	Workload	+	+	+
	Traffic complexity	+	+	+

Notes: "+" indicates that two indexes are correlated.

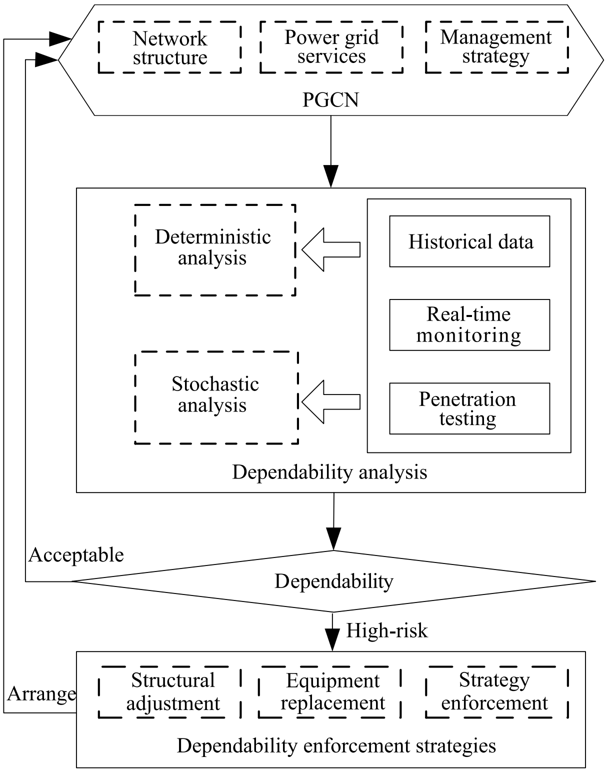

Fig. 5 Services-based dependability model of PGCN.

policies are necessary parameters to construct a proper model. The value of dependability is computed by adopting deterministic and stochastic analysis methods. As it does not meet the dependability requirement, finding an improvement strategies is necessary.

With the development of dependability model, dependability analysis shall be a necessary work for running PGCNs, and it should attempt to beforehand find vulnerability, security risks, and trend predication according to various information. The model may be used in the following stages: deploying new services, updating PGCNs, common operation, and emergency response. When planning a deployment policy for power grid services, the model aims to determine interdependence among them and the optimal strategy. For the common operation, studying status of PGCN and enhancing resource utilization can achieve by the model. Using the model might improve efficiency of emergency response when some events happen. We analyze dependability of PGCN by penetrating two kinds of failure patterns like Fig. 1. The first describes that a power grid event stimulates many services and PGCN receives a burst traffic request. Finding the bottleneck is its primary goal. The second indicates some components of PGCN were broken and might result in power grid service out of work and power grid outage. Determining how scale of the power grid is affected is its primary goal. We give respectively deterministic and stochastic methods to deal with the above two cases.

3.2 Constructing dependability model

In this part, we introduce two methods constructing the dependability analysis model of PGCN: the matrix model and Petri nets model.

3.2.1 Matrix model

Given a PGCN, denoted with G, where nodes represent communication sites or devices and edges represent communication lines. For one power grid service, its communication strategy is a sub-graph of G. Figure 6 models a PGCN and two services' communication strategies (the primary 1-2-3-6 and the secondary 1-4-5-6 are for service 1-6, the primary 2-5 and the secondary 2-1-4-5 are for service 2-5). We define the networking matrix and service matrix to represent the PGCN and its services respectively.

A PGCN G with n sites can be described as an $n \times n$ matrix, where entity $e_{ij} = 1$ if there exists an edge between nodes i and j or the device is well if $i = j$. We call the matrix networking matrix. Formally, for $1 \leqslant i, j \leqslant n, e_{ij} = 1$ means there exists a direct communication line between i and j, and $e_{ij} = 0$ indicates there is no lines between i and j or the line fails. Then if a failure happens, the networking matrix should update according to the following specifications: If $i - j$ breaks, then the resulting matrix $\boldsymbol{G}' = [e']$ is obtained through: (1) $e'_{ij} = e'_{ji} = 0$; (2) $e'_{mm} = e_{mm}$; (3) $e'_{mk} = e'_{km} = e'_{mm}e'_{kk}e'_{mk}$, where for $1 \leqslant k, m \leqslant n$. A communication strategy matrix is obtained by the following stages: If a service has one primary and x secondary predetermined paths, node i is used in the above paths, then $e_{ii} = 1$. For the primary path, if $i - j$ belongs to it, then $e_{ij} = 1$. For a secondary path numbered the k-th, $a_0 - a_1 - \cdots - a_{k-1} - a_k$, $e_{ij} = 1$ if $e_{xj} = 0$ for $x \neq j$ or $e_{ij} = 1$, otherwise, $e_{ij} = 1(k)$. Any failure shall update the matrix, and the updating speciation is same as the networking matrix.

For above example, we obtain the matrix models as follows.

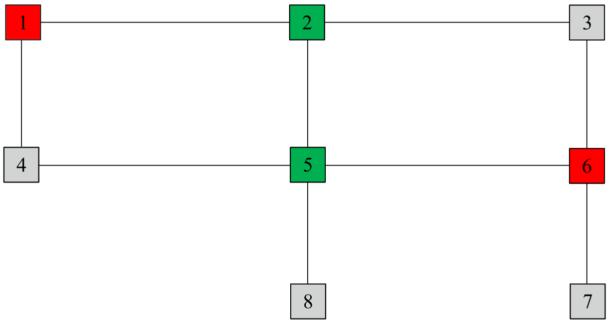

Fig. 6 An example of PGCN and communication strategy of power grid services. The services are 1-6 and 2-5, 1-2-3-6 and 1-4-5-6 are the strategy for service 1-6; 2-5 and 2-1-4-5 are strategy for service 2-5.

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

$$\boldsymbol{T}_{2\text{-}5} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

$$\boldsymbol{T}_{1\text{-}6} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Assuming the site 4 fails, $\boldsymbol{T}_x(Y)$ represents the matrix of the service x under the failure Y. For above example, we get the following matrices.

$$\boldsymbol{T}_{1\text{-}6}(4) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$\boldsymbol{T}_{2\text{-}5}(4) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Based on the obtained matrices, we could analyze PGCN's dependability and discuss them in the following parts.

3.2.2 Petri nets model

Let $\mathbf{N}$ be natural number set and $\mathbf{N}^+$ be positive natural number set. Stochastic Petri Nets (SPN) is a six-tuple SPN $= \{P, T, \mu, F, W, M_0\}$, where P is the place set, T is the transition set, and $\mu(t)$ is the firing rate of transition t (if the value is infinite, the transition t is called immediate one, otherwise it is called timed one). $F \subseteq (P \times T) \cup (T \times P)$ is arc set. $W : F \rightarrow \mathbf{N}^+$ is weight function set of arcs. $M : P \rightarrow \mathbf{N}$ is the marking, and M_0 is the initial marking. For $x \in P \cup T$ we set $^{\cdot}x = \{y|(y,x) \in F\}$ and $x^{\cdot} = \{y|(x,y) \in F\}$. $x \in T$ shall fire if the element $*$ in $^{\cdot}x$ has more than $W(*,t)$ tokens. After x fires, the marking is changed as $M(p) = M(p) - W((p,t)) + W((t,p))$. In SPN model, places and tokens are separately drown as circles and black dots, timed and immediate transitions are denoted by boxes and bars respectively, and the arc weight function is marked on the arc.

By the previous analysis, the communication line failures will cause services running on this line break, communication site failures cause that multiple devices locating in it could not work well. The following SPN model could reflect the above fact, as shown in Fig. 7.

S_{up} and S_{down} denote the normal state and failure state of the site respectively. T_{sud} and T_{sdu} denote failing and repair process of the site respectively. Similarly, E_{up}, E_{down}, T_{Eud}, T_{Edu} and L_{up}, L_{down}, T_{Lud}, T_{Ldu} denote the failing and repair scenarios of equipment and line respectively. The immediate transition reflects their relationships. The interdependence between communication infrastructure and power grid services is modeled as follows: Failures of communication infrastructure affect the running of services, taking the line failure for example, if the performing service T depends on the line, their relationship can be described as shown in Fig. 8.

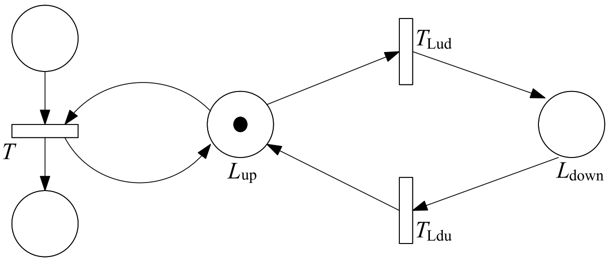

Fig. 7 SPN model of failure and repair of components in the PGCN.

Given a service, we can obtain its SPN model stage by stage like Fig. 9. The relationship among stages is described by the serial structure. The detailed stage model is obtained according to the design of strategies. Also, transition C_{ij} represents a service passing the line or communication equipment.

For a service, the strength of traffic affects mainly the dependability of PGCN, and the traffic model could be obtained by the following process. Traffic generating to PGCN consists of two aspects: the first traffic and the repeated traffic. Consider the effect of the environment, we can describe it as the following model shown in Fig. 10.

Transition T_{PJ} represents generating traffic. To describe the fact that the traffic is processed in parallel, we model a lot of traffic flows in parallel.

3.3 Deterministic analysis

For availability, the aim is to determine whether a service works well under given failures, and how scale

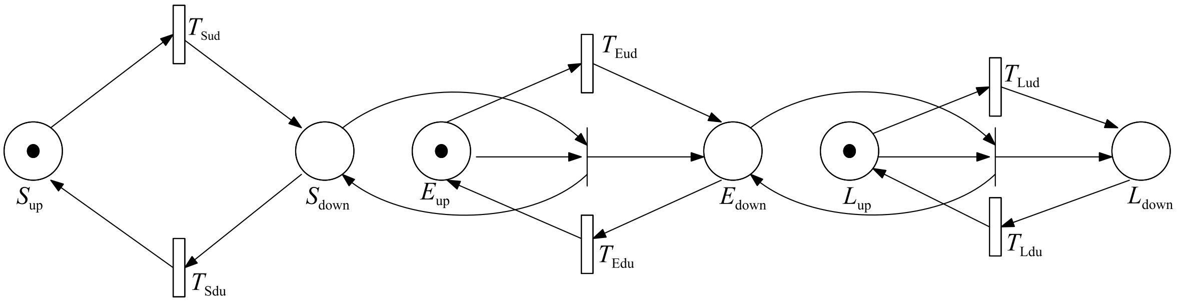

Fig. 8 Model of interdependence between service and PGCN.

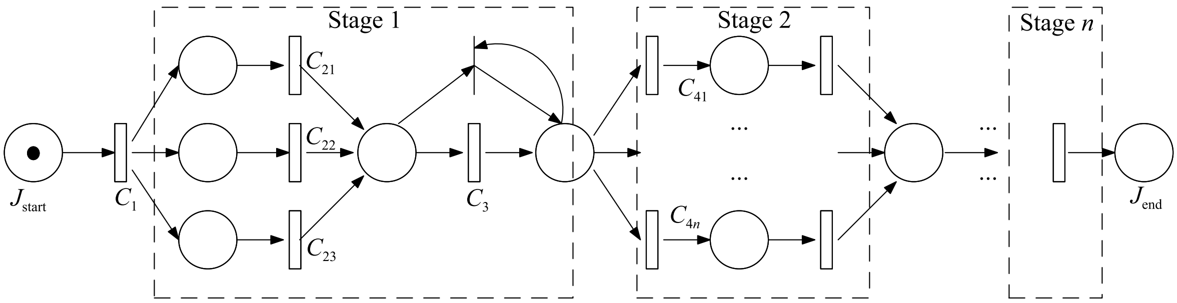

Fig. 9 SPN model of service process.

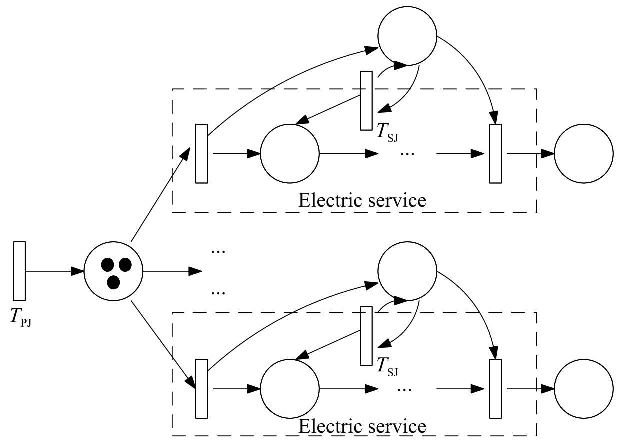

Fig. 10 SPN model about traffic generation of services.

Algorithm 1 Judge whether failures affect services

```
Input: $T_x(Y) = [e_{ij}]$ is the matrix of service $x$ after failure $Y$, $A$ and $B$ are sets of source nodes and terminal nodes, and $V$ is the set of nodes used in service $x$.
Output: Whether the service works?
1. Judge whether there is live path between $a$ and $b$, where $a \in A, b \in B$:
  1.1 If there is no $e_{ak} = 1$,where $k \neq a$ and $k \in V$, there is no channel between $a$ and $b$; otherwise, if $e_{af} = 1$, let $I = a$, get into 1.2
  1.2 Let $e_{vI} = 0$, where $v \in V$. If $f = b$, there is the channel between a and b; otherwise, if there is no $e_{fk} = 1$, where $k f$ and $k \in V$, get into 1.1; otherwise, if $e_{af} = 1, I = f$, get into 1.1
2. Judge whether a service works
  2.1 Test each predetermined path using method 1.
  2.2 If there has no path supporting the service, the service outage; otherwise, the service is ok.
```

of services does a failure affect?

For data quality, if we know that the quality is determined by the number of available paths (e.g., the quality is $\log^{(x+1)}_{(d+1)}$, where x is the current available paths and d is predetermined number of paths), the aim is to judge whether the quality is ensured under given failures.

For maintainability, we judge it by the fault tolerance of PGCN, i.e., how many number of failures does the given strategy endure?

3.4 Stochastic analysis

Stochastic analysis is also called dynamic analysis. For dependability, we shall analyze the stable distribution of system states, Mean Time To Breach (MTTB), and MTTR and determine the most likely failure in the near future.

MTTB reflects the availability of the system, which has been widely studied in reliability engineering. In our model, we focus on the MTTB for all kinds of special traffic, a service, and the whole system.

MTTR reflects the efficiency of the system to deal with failure and should include the time of finding and repairing failures.

Estimating possible threat is another important task for stochastic analysis, and the state analysis will support this task.

4 Dependability Analysis of PGCN

4.1 Matrix-based analysis

4.1.1 Key nodes/ key lines

Given a service matrix, using Algorithm 1, we can easily judge whether the service works well. The possible of component failure is various with respect to device types, location, management level, and so on. The workload of service components supporting is different. We call a component the key one if the metric value exceeds a given threshold. The metric and threshold are selected individually. In this paper, we just choose the metric as the product of failure possibility and supported traffic magnitude. In detail, given a component C, the metric value IC = FC × TC, where FC is failure possibility of C and TC is traffic magnitude. For simplicity, we adopt the normalization value, i.e., $\widehat{I_{\rm C}} = I_{\rm C}/D$, where D is the total number of services supported by this component. Different weights reflect the primary and the secondary paths. Simply, if 1 is the weight of the primary path of services, set $1/2$ be the weight of the second and $1/n$ be the n-th weight.

Now we will propose an algorithm to determine key components. Different services have different importance, so the corresponding traffic is set high, medium, and low levels. Their weight satisfy $W_{\rm h} > W_{\rm m} > W_{\rm l}$. Given failure pattern A, T_v denotes affected traffic set, let $C(A)$ and $\overline{C(A)}$ be the sum influence and mean influence of A, then

$$C(A) = \sum_{t \in T_v} W(t),$$

$$\overline{C(A)} = \sum_{t \in T_v} W(t)/|T_v|.$$

Suppose the failure probability of A is known, we obtain the expectation of influence as follows:

$$C'(A) = C(A) \times P \;\text{ and }\; \overline{C'(A)} = \overline{C(A)} \times P,$$

where $P = \prod_{a \in A} \mathrm{pr}(a)$ and $\mathrm{pr}(a)$ is the probability of failure a.

We call the failure pattern A the key component of PGCN if its influence value is larger than a fixed threshold, $\boldsymbol{U}$, and $|A| \leqslant L$, where L is a fixed integer. Based on Algorithm 1, we obtain Algorithm 2 to find the key components as follows.

4.1.2 Generating emergency response strategies

Through adopting matrix to represent PGCN, current status of the PGCN after any failures happened could be represented by modifying the value of elements in this matrix (the detail refers to Section 3.2). Here we present an shortest path distance based algorithm.

In fact, for the given service set T, it is easy to construct an ancillary matrix $\boldsymbol{G}' = [e'_{ij}]$ based on networking matrix $\boldsymbol{G} = [e_{ij}]$ and service matrix set $\boldsymbol{A}^f = [a^f_{ij}]$ as follows: (1) If $a^f_{ij} = 1(k)$, let $a^f_{ij} = k$ and $e'_{ij} = \sum_f a^f_{ij}$; (2) If $e'_{ij} = 0$, let $e'_{ij} = \infty$.

For the service t, we can obtain a communication strategy by adopting Dijkstra algorithm on the matrix $\boldsymbol{N}'$. The detailed algorithm is shown in Algorithm 3.

Algorithm 2 Analysis of the key component of system

Input: Networking matrix N, service set T and its matrix $T_x = [e^x_{ij}], x \in T$.

Output: The set of the key components

```
1. Generation of the failure pattern (or key component candidates) Based on $N$, the failure set is generated as the following rules:
   (1) $e_{ij} = 1$ implies nodes $i, j$ and edge $i - j$ is the candidate elements
   (2) Fix an upper bound $L$, constructing $C_n^{\ell}$ subset of candidate set, where the number of elements in any subset is no more than $L$.
   (3) Reduce candidates: if $A$ is a candidate and $(i \in A \bigvee j \in A) \bigwedge (e_{ij} \in A)$ is true, then updated candidate $A' = A/\{e_{ij}\}$. Let the candidate set be $Ask$.
2. Increasingly calculate influence $C(A)$ or $\overline{C(A)}$ of failure pattern $A$ with respect to the number of elements in it
   2.1 Determine the affected service set $T_v(A)$ using Algorithm 1;
   2.2 Calculate $C(A)$ or $\overline{C(A)}$
3. Find the set of the key component
   3.1 If $C(A)$ or $\overline{C(A)}$ is greater than the fixed constant, then the $A$ is a key component ;
   3.2 If $A$ is a key component set, the delete candidate $B$, if $A \subset B$;
   3.2 If $Ask$ is not empty, go to step 2, otherwise output all key component set
```

Algorithm 3 Design of minimum load path of service

Input: Auxiliary matrix N', the failed service set T_v.

Output: Communication strategies of failed services

```
1. Given a service $T$, construct strategy candidates
   1.1 Splitting T as the union of subservice that has one source to multiple destinations, i.e. $t_{x1D_1} \cup t_{x_2D_2} \cup \ldots \cup t_{x_pD_p}$, where $|x_i| = 1$ and $|D_i| \geqslant 1$.
   1.2 Construct feasible communication strategy of $t_{x_iD_i}$ using Dijkstra algorithm:
      1.2.1 For $i < p$, construct strategy of $t_{x_iD_i}$ by Dijkstra algorithm and generate the corresponding service matrix;
      1.2.2 Update auxiliary matrix $\boldsymbol{N}'$ after adding service matrix $t_{x_iD_i}$, into $A$, let $i = i + 1$ and go to 1.2.1
      1.2.3 If $i = p$, construct strategy of $t_{x_pD_p}$ and update $\boldsymbol{N}'$
      1.2.4 Collect strategies
2. Judge feasibility of strategies
   2.1 Select key components as failure pattern, using Algorithm 1 to judge the proposed strategies;
   2.2 If a strategy is affected, update $\boldsymbol{N}'$ through considering the failure pattern and go to 1; otherwise go to 2.1;
   2.3 Output strategies
```

4.2 SPN-based analysis

4.2.1 Construction of SPN

For evaluating and designing specific strategies, the following steps are necessary to be used to construct the proper models.

Step 1 Collecting all power grid services and building communication service models using the method in Section 3.2. For given components including lines and sites, model them with places. The service process is modeled from one place to another, and the transition between them reflects the capability of its precedent component.

Step 2 Setting traffic generation modular. According to service pattern modeled in Fig. 4, constructing traffic generation modular and connecting to corresponding places of devices. Please see Fig. 10 for constructing traffic SPN.

Step 3 Modelling failure mode and combining models. We simply regard any device has just two states: UP and DOWN, the failure model is represented by splitting the corresponding device place into two places, one represent UP and the other is DOWN. They are connected with transitions shown in Fig. 9.

Step 4 Setting parameters and evaluating dependability of systems. The historical statistic data and experience determine the setting of parameters, we discuss it in the next. The content of dependability analysis is discussed in Section 3.4 and the corresponding methods refer to Ref. [2].

For the example shown in Fig. 6, we obtain the model shown in Fig. 11 using methods from Steps 1-3. Two services traffic are generated by transitions J_{16} and J_{25}. Failure models of sites 1 and 2 describe the failure pattern.

4.2.2 Determining parameter value

The value of parameter impacts the accuracy and validity of results. Here we just discuss the principle determining parameters including fire rates and initial marking.

(1) The selection of the stochastic function of transition occurring

In our model, transitions are separated into traffic processing transition, traffic generation transition, and failure pattern transition.

For the first two kinds of transitions, the selected stochastic function should realize tradeoff between solvability and correctness. The effect factors include length of line, the type of equipment/service, location environment, and management level. Generally, the average waiting time is inversely proportional with factors mentioned above.

For failure pattern transition, the average waiting time is related to external environment, management level, and its individual attributes.

(2) Initial marking

Initial marking is an important factors impacting the results’ accuracy, especially for transient analysis. Initial marking of SPN model represents the state of system at the beginning of observation. Token distribution in places denoting DOWN represents a special failure pattern. To analyze devices performance, we always put enough tokens in the traffic generation places.

4.2.3 Dependability analysis based on SPN

Steady analysis and transient analysis could be developed by SPNs. The common method includes the following steps transforming SPN to a stochastic process, computing steady/transient distribution of states, and analyzing dependability. Many literature comprehensively discussed it (see Ref. [2]), in this paper, we shall omit the detailed calculation process and just propose how to determine dependability representation in SPNs.

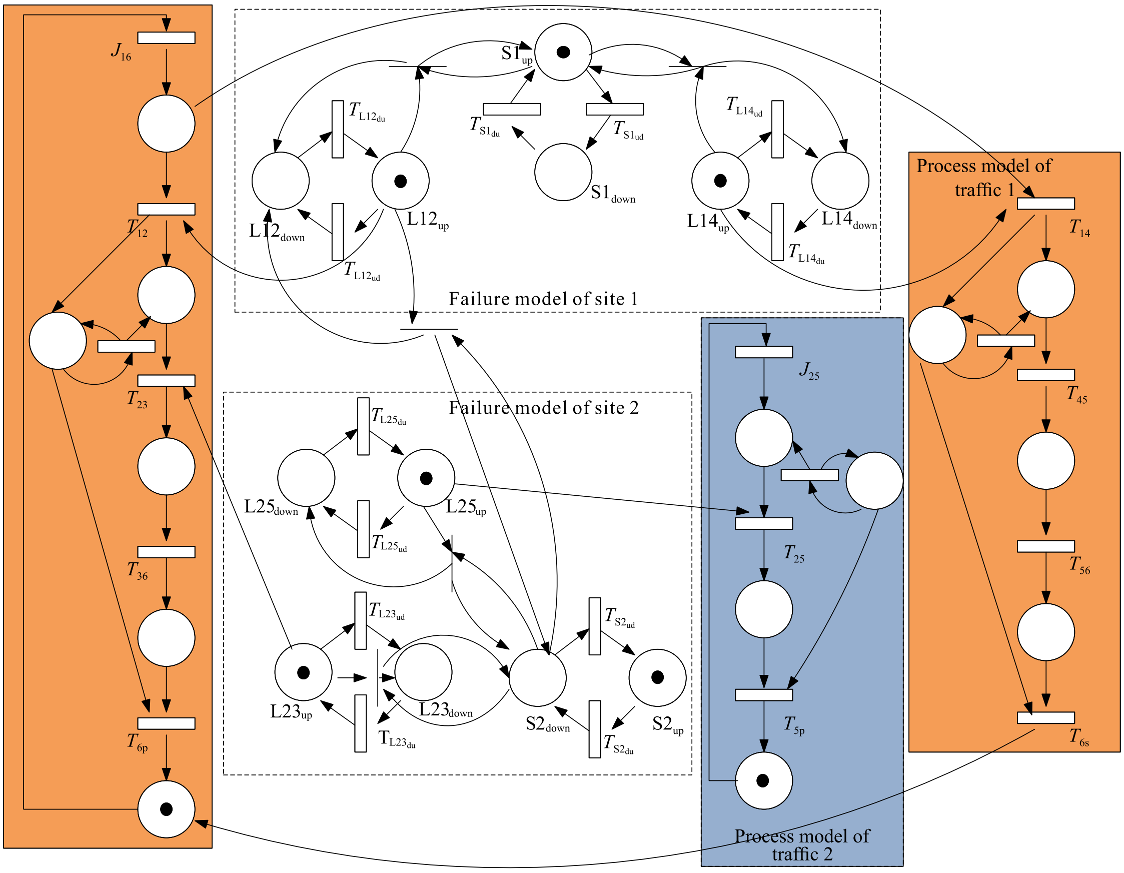
J_{16}
T_{12}
T_{23}
T_{36}
T_{6p}
$\mathrm{S1}_{\mathrm{up}}$
T_{S1du}
T_{S1ud}
$\mathrm{S1}_{\mathrm{down}}$
T_{L12du}
$\mathrm{L12}_{\mathrm{down}}$
$\mathrm{L12}_{\mathrm{up}}$
T_{L12ud}
T_{L14ud}
$\mathrm{L14}_{\mathrm{up}}$
$\mathrm{L14}_{\mathrm{down}}$
T_{L14du}
Failure model of site 1
Process model of traffic 1
T_{14}
T_{45}
T_{56}
T_{6s}
Failure model of site 2
T_{L25du}
$\mathrm{L25}_{\mathrm{down}}$
$\mathrm{L25}_{\mathrm{up}}$
T_{L25ud}
T_{L23ud}
$\mathrm{L23}_{\mathrm{up}}$
$\mathrm{L23}_{\mathrm{down}}$
$\mathrm{T}_{\mathrm{L23du}}$
T_{S2ud}
$\mathrm{S2}_{\mathrm{down}}$
$\mathrm{S2}_{\mathrm{up}}$
T_{S2du}
J_{25}
T_{25}
T_{5p}
Process model of traffic 2

Fig. 11 SPN model of dependability analysis of the example in Fig. 6.

Given a service, applying Algorithm 1 we can determine a set of failure pattern denoted by F, which makes this service outage. We apply the following technique to reduce F: if $A, B \in F$ and $A \subset B$, then delete B from F, and denote the reduced set F'. We denote $M(f) = 1$ if the marking satisfies the following condition: The corresponding places of f all have at least one token under the marking M, which implies service outage. Let $\widehat{t} = \min_M\{t \mid \bigvee_i M(f_i) = 1\}$ and $\widetilde{t} = \min_M\{t \mid \bigwedge_i M(f_i) = 0\}$, thus, for transient analysis,

$$\mathrm{MTTB} = t - t_0,$$

where t_0 is the beginning time, and

$$\mathrm{MTTR} = \widetilde{t} - \widehat{t}.$$

For steady analysis, the marking set such that $\bigvee_i M(f_i) = 1$ means the service outage, the marking set such that $\bigwedge_i M(f_i) = 0$ reflects the service works well, and the equivalent transforming rates between them can be used to determine the value of MTTB and MTTR.

5 Conclusions

Dependability analysis is used extensively in computer networking and complicated systems. PGCN plays more and more critical role. However, the results of its dependability analysis show that there lack dependability models considering the interdependence between information infrastructure and power grid infrastructure. Based on analysis of smart grid PGCN's structure, power services' communication pattern, and dependability impact factors, we present its dependability metrics and obtain a power grid services based dependability model of PGCN. Our model includes modular of model construction, model analysis, and fault response. We discuss two kinds of analysis methods, the deterministic and the stochastic, and provide two analysis techniques respectively. The matrix-based analysis promotes the efficiency of finding key components (the important failure patterns) and designing fault response strategies. For SPN method, we study several techniques to model the problem in fine-grained and give dependability definitions based on SPNs. The proposed methods shall be verified through real operation in SGCC.

Acknowledgements

This work was supported by the National Key Basic Research and Development (973) Program of China (No. 2010CB328105), the National Natural Science Foundation of China (Nos. 61020106002, 61071065, and 11171368), China Postdoctoral Science Foundation (No. 2013M540952), Tsinghua University Initiative Scientific Research Program (No. 20121087999) and SGCC research and development projects.

References

[1] IEEE Standard Glossary of Software Engineering Terminology, IEEE Standard 610.12-1990, https://standards.ieee.org/findstds/standard/610.12-1990.html, 2014.

[2] R. Zeng, Y. X. Jiang, C. Lin, and X. M. Shen, Dependability analysis of control center networks in smart grid using stochastic petri nets, *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1721-1730, 2012.

[3] USA Department of Energy, Smart Grid / Department of Energy, http://energy.gov/oe/technology-development/smart-grid, 2014.

[4] R. R. Rajkumar, L. Insup, S. Lui, and J. Stankovic, Cyberphysical systems: The next computing revolution, in *Proceedings of the 47th Design Automation Conference*, ACM, Anaheim, USA, 2010, pp. 731-736.

[5] G. N. Ericsson, Cyber security and power system communication-essential parts of a smart grid infrastructure, *Power Delivery, IEEE Transactions on*, vol. 25, no. 3, pp. 1501- 1507, 2010.

[6] Y. Mo, T. H. H. Kim, K. Brancik, and D. Dickinson, Cyber-physical security of a smart grid infrastructure, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, 2012.

[7] S. Sridhar, A. Hahn, and M. Govindarasu, Cyber-physical system security for the electric power grid, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012.

[8] S. M. Amin and B. F. Wollenberg, Toward a smart grid: Power delivery for the 21st century, *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34-41, 2005.

[9] K. Moslehi and R. Kumar, A reliability perspective of the smart grid, *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 57-64, 2010.

[10] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, Communication network architecture and design principles for smart grids, *Bell Labs Technical Journal*, vol. 15, no. 2, pp. 205-227, 2010.

[11] J. C. Laprie, K. Kanoun, and M. Kaaniche, Modelling interdependencies between the electricity and information infrastructures, in *Computer Safety, Reliability, and Security*, F. Saglietti and N. Oster, Eds. Springer, 2007, pp. 54-67.

[12] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, *Control Systems, IEEE,* vol. 21, no. 6, pp. 11-25, 2001.

[13] R. Berthier, R. Bobba, M. Davis, K. Rogers, and S. Zonouz, State estimation and contingency analysis of the power grid in a cyber-adversarial environment, http://csrc.nist.gov/newsevents/cpsworkshop/slides/presentation-9berthier-bobba-davisrogers-zonouz.pdf, 2014.

[14] D. Niyato, P. Wang, and E. Hossain, Reliability analysis and redundancy design of smart grid wireless communications system for demand side management, *Wireless Communications, IEEE,* vol. 19, no. 3, pp. 38-46, 2012.

[15] S. Jih and M. L. Yin, An availability analysis on SONET ring networks in power grid communications, in *Reliability and Maintainability Symposium (RAMS), 2012 Proceedings-Annual, IEEE*, Reno, USA, 2012, pp. 1-6.

[16] C. Quinn, D. Zimmerle, and T. H. Bradley, The effect of communication architecture on the availability, reliability, and economics of plug-in hybrid electric vehicle-to-grid ancillary services, *Journal of Power Sources*, vol. 195, no. 5, pp. 1500-1509, 2010.

[17] A. Z. Faza, S. Sedigh, and B. M. McMillin, Reliability analysis for the advanced electric power grid: From cyber control and communication to physical manifestations of failure, *Lecture Notes in Computer Science*, vol. 5775, pp. 257-269, 2009.

[18] H. A. Rahman, K. Beznosov, and J. R. Marti, Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports, *International Journal of Critical Infrastructures*, vol. 5, no. 3, pp. 220-244, 2009.

Jiye Wang received the PhD degree in electrical engineering from Tsinghua University, China in 2007. Currently, he is a professor-level senior engineer, deputy director of SGCC Information and Communication Department. His research interests include information management of power systems, smart grid, and the next generation energy system.

Kun Meng received the PhD degree in communication and information system from University of Science and Technology Beijing, China, in 2012. Currently, he is a postdoctor fellow of the Department of Computer Science and Technology at Tsinghua University. His research interests include energy internet, wireless networking, performance evaluation, network security, and stochastic models. Dr. Meng is a member of CCF and ACM.

Junwei Cao received his PhD degree in computer science from the University of Warwick, Coventry, UK, in 2001. He is currently a professor and deputy director of Research Institute of Information Technology, Tsinghua University, China. He is also the director of Open Platform and Technology Division, Tsinghua National Laboratory for Information Science and Technology. He has published over 150 papers and cited by international scholars for over 6000 times. He has authored or edited 6 books. His research focuses on distributed computing technologies and applications. Prof. Cao is a senior member of the IEEE Computer Society and a member of the ACM and CCF.

Zhen Chen is an associate professor in Research Institute of Information Technology at Tsinghua University. He received his BEng and PhD degrees from Xidian University in 1998 and 2004. He once worked as postdoctoral researcher in Network Institute of Department of Computer Science at Tsinghua University during 2004 to 2006. He was also a visiting scholar in UC Berkeley ICSI in 2006. His research interests include computer network security, trustworthy computing and performance evaluation. He has published around 80 academic papers.

Lingchao Gao is currently a senior engineer of SGCC Information and Communication Department. He received the BS degree from Henan University, China, in 1994. His research interests include information management of power systems, smart grid, and the next generation energy system.

Chuang Lin received the PhD degree in computer science from Tsinghua University, China, in 1994. Currently, he is a professor of the Department of Computer Science and Technology, Tsinghua University. His research interests include computer networks, performance evaluation, network security analysis, and petri net theory and its applications. Prof. Lin is a member of CCF, IEEE, and ACM, as well as a steering committee member of International Petri nets group, and the fellow of CCF.